CLAIMS

1. A system arranged to provide a gateway between a first network and a second network, the system comprising:

interface means to receive from the first network a message intended for an object in the second network, the message including an identifier for a further object in either the first or second network;

means to generate further interface means for receiving from the second network messages for the further object;

means to form a new identifier for the further interface means;

means to replace the received identifier with the new identifier in the message; and

means to forward the message to the object in the second network.

2. A system according to claim 1, wherein the new identifier includes information to enable subsequent recovery by the system of the received identifier.

3. A system according to claim 2, wherein the new identifier includes a representation of the received identifier.

4. A system according to claim 2, wherein the new identifier includes an indication of the identity of the received identifier and the system includes means to associate said indication with said received identifier.

5. A system according to ~~any one of the preceding claims~~ Claim 1, comprising means to include in the new identifier a name tag to identify the interface means.

6. A system according to ~~any one of the preceding claims~~ Claim 1, comprising means to include in the new identifier check data for checking the validity of the or at least a part of the new identifier.

7. A system according to claim 6, wherein the check data comprises the result of a hash operation on the, or the at least part of the, new identifier and a secret.

8. A system according to ~~any one of the preceding claims~~ Claim 1, comprising means to include in the new identifier an indication that the received identifier was received in an message from the first (or second) network.

9. A system according to claim 1, comprising means to determine whether the received identifier originated from the first network or the second network.

10. A system according to claim 9, comprising means to form the new identifier on the basis of the determined origin.

11. A system according to claim 10, wherein, if the received identifier originated in the first network, the means to form the new identifier forms a new identifier including information to enable subsequent recovery by the system of the received identifier.

12. A system according to claim 10, wherein, if the received identifier originated in the second network, having passed through the system from the second network to the first network, the means to form the new identifier forms a new identifier comprising an original identifier recovered from information included in the received identifier.

13. A system according to claim 10, wherein, if the received identifier originated in the first network, having passed through the system from the first network to the second network and having passed back to the first network other than through the system, the means to form the new identifier forms the new identifier as a copy of the received identifier.

14. A system according to claim 1, comprising means to detect a name tag in the message.

15. A system according to claim 14, comprising means to determine on the basis of the name tag whether the object in the second network is valid and is still available to receive messages.

16. A system according to claim 15, wherein the means to determine initiates a call to a naming service, the naming service being configurable by an authorised party by adding or removing name tags, and the presence or absence of a name tag being indicative of whether the object associated with the name tag is available or not respectively.

17. A system according to claim 1, comprising means to verify the received identifier.

18. A system according to claim 17, wherein identifier includes check data to enable verification of the received identifier.

19. A system according to claim 18, wherein the check data is the result of a hash operation enacted

on at least part of the identifier and a secret, and the means to verify the received identifier is configured to enact a similar hash operation on the same part of the identifier and a secret and compare the resulting check data with the received check data.

20. A system according to claim 19, wherein the secret is stored by and only accessible by the gateway.

21. A system according to claim 1, wherein the means to generate the further interface means comprises means to determine on the basis of the received identifier whether a template for an appropriate further interface means is already known to the system.

22. A system according to claim 21, wherein the means to generate the further interface means comprises means, which is operable in the event an appropriate template is not known to the system, to obtain an appropriate template from a remote repository.

23. A system according to claim 21 ~~or claim 22~~, wherein the means to generate the further interface means comprises means, which is operable in the event no appropriate template is known to the system and/or an appropriate template is not recoverable from a remote repository, to obtain a generic template.

24. A system according to ~~any one of claims 21 to 23~~ Claim 21, wherein the means to generate the further interface is arranged to at least obtain a template for the further interface means on or after receipt of the received identifier and in advance of receipt of a message for the further object.

25. A system according to ~~any one of the preceding claims~~ Claim 1 configured for operation in a trusted operating system.

26. A system according to claim 25, wherein the trusted operating system enforces Mandatory Access Control.

27. A system according to claim 26, comprising at least two logical compartments and a trusted relay process that has privileges necessary to pass messages between the two compartments, wherein the first network and the respective interface means are associated with a first compartment and the second network is associated with a second compartment.

28. A system according to claim 26 ~~or claim 27~~, wherein a secret, usable by the system in a hash

operation for validating object references, is associated with a third compartment, and wherein only the trusted relay process has the privileges necessary to retrieve the secret from the further compartment in order to enact a hash operation.

29. A system according to claim 1, wherein the received identifier is an Interoperable Object Reference having the form IOR[host: port: key].

30. A system according to ~~any one of the preceding claims~~ claim 1, wherein the new identifier is an Interoperable Object Reference having the form IOR[host x: port x: key x], wherein key x includes information to enable subsequent recovery by the system of the received identifier.

31. A system according to claim 30, wherein key x includes a representation of the received object reference IOR[host i: port i: key i].

32. A system according to claim 30 ~~or claim 31~~, wherein key x includes:

an identifier to indicate from which network the object reference originated;

a name tag associated with an identity of the gateway process; and

check data for verifying the validity of the object reference.

33. A method of controlling a gateway to pass messages for objects between first and second networks attached to the gateway, the method comprising the steps of:

receiving from the first network a message for an object in the second network, the message including an identifier for a further object in either the first or second network;

generating means to receive messages for the further object;

forming a new identifier for the means to receive messages for the further object;

replacing the received identifier with the new identifier in the message; and

forwarding the message to the object in the second network.